401 – MSN Session Logs and Chat

Team Information

Team Name: Barely Legal

Results Email: [redacted]

Examination Time Frame: to 10/31/08

Instructions

Description: Examiners must develop and document a methodology used to parse MSN Session Logs and Chat communications from the presented MSN Chat program files contained in the folder **401_MSN_Session_Logs_and_Chat_Challenge2008** to an easily understandable and readable format. The supplied files were from either or both of the two computers used in the chat conversation. A detailed explanation of your process (software or technique) used to examine, extract, and present the data is required. A detailed explanation of your process (software or technique) used to examine, extract, and present the data is required.

Points will be awarded for the completeness of the data recovered from the communications and the ease of understanding or utility of the method the information is reported from that file(s).

Total Weighted Points: 80 Total Points available per entry – Total 400 Points Available

1. **Answers** – Fill in the chart below with your findings. *As a Forensic Challenge, consider that your answers will have to have enough detail for the Findings and Methodology of your examination to satisfy questioning in a court of law.*
2. **Methodology** – Provide a meticulously detailed explanation of your process. Be sure to include a step action that our reviewers can follow to reproduce your work for authenticity including tools and techniques.

Internal Reviewer Use Only

Reviewer: Points Awarded:

Date: Review Period: to

Completed: ☐ Yes ☐ No ☐ Partial

REPORT OF EXAMINATION

401 – MSN Session Logs and Chat

Three conversation logs were recovered and extracted from the "401_MSN_Session_Logs_and_Chat_Challenge2008" folder. All located in the "MSN 1\MSN Messenger\My Received Files\yogibear19534226628795\History" folder, the chat logs were:

```
yogibear19322121292544.xml
yogibear19534226628795.xml
udorntani1744684863.xml
```

The reformatted contents are shown below:

(yogibear19322121292544.xml)

```
Date="4/3/2008" Time="10:26:24 AM"
From: bob     To: yogibear1953@hotmail.com
back yet

Date="4/3/2008" Time="10:26:35 AM"
From: yogibear1953@hotmail.com    To: bob
not yet

Date="4/3/2008" Time="10:28:02 AM"
From: bob     To: yogibear1953@hotmail.com
have to go for a minute

Date="4/3/2008" Time="10:28:16 AM"
From: yogibear1953@hotmail.com    To: bob
ok

Date="4/3/2008" Time="10:52:01 AM"
From: bob     To: blane
BACK YET?????

Date="4/3/2008" Time="10:52:28 AM"
From: blane   To: bob
no hold on will you

Date="4/3/2008" Time="11:18:21 AM"
From: bob     To: blane
you back yet

Date="4/3/2008" Time="11:59:06 AM"
From: blane   To: bob
hey im back you ther?

Date="4/3/2008" Time="11:59:13 AM"
From: blane   To: bob
hey im back man

Date="4/3/2008" Time="11:59:16 AM"
From: blane   To: bob
hey you on
```

Date="4/3/2008" Time="11:59:28 AM"
From: bob To: blane
yea i was on the can man

Date="4/3/2008" Time="11:59:31 AM"
From: blane To: bob
ok

Date="4/3/2008" Time="11:59:44 AM"
From: bob To: blane
everything good on your enc?

Date="4/3/2008" Time="11:59:58 AM"
From: blane To: bob
yea its ready im ready you?

Date="4/3/2008" Time="12:00:16 PM"
From: bob To: blane
Good, I tested out my specialo black powder cake and man oh man

Date="4/3/2008" Time="12:00:36 PM"
From: blane To: bob
You didn't blow it all did you?

Date="4/3/2008" Time="12:01:03 PM"
From: bob To: blane
I aint that stupid Blaine

Date="4/3/2008" Time="12:01:17 PM"
From: blane To: bob
Hey, you said no names

Date="4/3/2008" Time="12:02:12 PM"
From: bob To: blane
Sorry, were even then. Listen I took a handful of the stuff, put in in that metal pipe with the ball berrings glued all over and went down to the dump at night.

Date="4/3/2008" Time="12:03:10 PM"
From: bob To: blane
Lit that bad mojo off and ran over the hill and dropped 'WHAM'. Took a quick look and what a hole and everything standing was shredded. What a ruswh.

Date="4/3/2008" Time="12:03:34 PM"
From: blane To: bob
So that's what thyre talkin about on the news this morning

Date="4/3/2008" Time="12:03:51 PM"
From: bob To: blane
News, what news? What u talking about?

Date="4/3/2008" Time="12:04:45 PM"
From: blane To: bob
It was all over the news, some kind of explosion at the dump was reported. They're checking to see if it as like natural gass or something or some junk somebody threw away

Date="4/3/2008" Time="12:04:52 PM"
From: bob To: blane
nuts

Date="4/3/2008" Time="12:05:29 PM"
From: blane To: bob
theyre going to figure this out man, that was a astupid play now they got the evidence

Date="4/3/2008" Time="12:05:52 PM"
From: bob To: blane
they don't have jack, all they got is a hole and some busted stuff

Date="4/3/2008" Time="12:06:46 PM"
From: blane To: bob
no, that was stupid. They got all this stuff to tell themn what is was and who made it. I watch those shows on tv about them CSI dudes and they always figure it out

Date="4/3/2008" Time="12:07:50 PM"
From: blane To: bob
whyd u have to do it so close to the city man, why not an out of state test

Date="4/3/2008" Time="12:24:54 PM"
From: bob To: blane
cause mom wouldn't let me have the car last noght and i couldn't drive it out of state even if I had it, no money for gas. So knock off htat stupid stuff I did what I could. Least I was smart enought and I tested it out and those tv shors are just that and a bunch of stuff too.

Date="4/3/2008" Time="12:26:23 PM"
From: blane To: bob
Man, I seen what they can do, theyre gonna find us and grill us till we give up the whole thing

Date="4/3/2008" Time="12:26:29 PM"
From: bob To: blane
That'

Date="4/3/2008" Time="12:27:57 PM"
From: bob To: blane
That's garbage so knock it off, well pull this, nobody finds us and were rich. Aint you tired of being poor, working for sucker money. Only way they get on to us is if you open your mouth and blab it all over

Date="4/3/2008" Time="12:28:48 PM"
From: blane To: bob
I don't rat, ut maybe we better not. Least not now.

Date="4/3/2008" Time="12:30:15 PM"
From: bob To: blane
It goes as planned and youre gonna be there too. I didn't spend all this time and effort for you to chicken out at the last nimute. If youre too yellow to work this with me ill get somebody else to pull it with. You just give me the guns and gear u got]

Date="4/3/2008" Time="12:30:55 PM"
From: blane To: bob
I aint no mor yellow thatn you. You think your so bad, just remember I can wip your tail anyday, did a year ago

Date="4/3/2008" Time="12:31:25 PM"
From: bob To: blane
Then your'e in?

Date="4/3/2008" Time="12:31:48 PM"
From: blane To: bob
You better believe it don't ever call me yellow again

Date="4/3/2008" Time="12:46:31 PM"
From: bob To: blane
Ok, need you like we planned tomorrow night outside the wharehouse. We go in while the guards are all at lunch, find the crates of ipods and get them out the door. Then we set the charges and get the stuff in the car and get out before the boom

Date="4/3/2008" Time="12:46:35 PM"
From: blane To: bob
What about the fuards

Date="4/3/2008" Time="12:46:44 PM"
From: blane To: bob
guards

Date="4/3/2008" Time="12:48:15 PM"
From: bob To: blane
If we stick to the schedule theyre still at lunc in the front of the building and with the walls the blast will never get them but all the evidence will be blasted. Nothing to point them at us and they'll figure the stuff we stole was deestroyed and probably wont even look for that stuff, just fugure gas blew or something

Date="4/3/2008" Time="12:48:23 PM"
From: blane To: bob
Man I hop your right

Date="4/3/2008" Time="12:49:17 PM"
From: bob To: blane
I am, and then we sell all those ipods for maybe 300 or 400 bucks each, couple of hundred of them, and figure the money with a 50 50 split. Lotta long green, keep you loaded a long time

Date="4/3/2008" Time="12:49:23 PM"
From: blane To: bob
Sweet

Date="4/3/2008" Time="12:49:48 PM"
From: bob To: blane
]So get a move on, I'll meet you there an hour before party time

Date="4/3/2008" Time="12:50:07 PM"
From: blane To: bob
Done, im outta here

Date="4/3/2008" Time="12:50:24 PM"
From: bob To: blane
Im gone too

(yogibear19534226628795.xml)

Date="4/3/2008" Time="11:53:16 AM"
From: Zeus To: blane
hey man whats up long time no talk

Date="4/3/2008" Time="11:53:40 AM"
From: blane To: Zeus
what are you talking about

Date="4/3/2008" Time="11:53:52 AM"
From: Zeus To: blane
just what i said

Date="4/3/2008" Time="11:54:22 AM"
From: blane To: Zeus
come on bob, quit horsing around, i know it's you.

Date="4/3/2008" Time="11:54:29 AM"
From: Zeus To: blane
ok, got me

Date="4/3/2008" Time="11:54:39 AM"
From: Zeus To: blane
just wanted to see if you'd bite

Date="4/3/2008" Time="11:55:07 AM"
From: Zeus To: blane
i switching back to normal sign on now

Date="4/3/2008" Time="10:52:01 AM"
From: bob To: blane
BACK YET?????

Date="4/3/2008" Time="10:52:28 AM"
From: blane To: bob
no hold on will you

Date="4/3/2008" Time="11:18:21 AM"
From: bob To: blane
you back yet

(udorntani1744684863.xml)

Date="4/3/2008" Time="11:53:16 AM"
From: Zeus To: blane
hey man whats up long time no talk

Date="4/3/2008" Time="11:53:40 AM"
From: blane To: Zeus
what are you talking about

Date="4/3/2008" Time="11:53:52 AM"
From: Zeus To: blane
just what i said

Date="4/3/2008" Time="11:54:22 AM"
From: blane To: Zeus
come on bob, quit horsing around, i know it's you.

Date="4/3/2008" Time="11:54:29 AM"
From: Zeus To: blane
ok, got me

Date="4/3/2008" Time="11:54:39 AM"
From: Zeus To: blane
just wanted to see if you'd bite

Date="4/3/2008" Time="11:55:07 AM"
From: Zeus To: blane
i switching back to normal sign on now

METHODOLOGY / NOTES FORM

401 – MSN Session Logs and Chat

Date / Time	Notes
26-Oct-08 2:30 pm	Tool(s) Used: Custom Perl script (attached with this report as file "401-clean.pl") Located MSN Chat Log files in the "MSN 1\MSN Messenger\My Received Files\yogibear19534226628795\History" directory. Created perl script (401-clean.pl) to extract and reformat relevant data.

```
#!/usr/bin/perl

#$thefile="udorntani1744684863.xml";
#$thefile="yogibear19322121292544.xml";
$thefile="yogibear19534226628795.xml";
open (FILE,"<$thefile");
@all_lines = <FILE>;
close FILE;

#$all_lines =~ s/<From/\n<From/g;

$thefile .= ".txt";
open (FILE,">$thefile");

foreach $line (@all_lines) {
$line =~ s/<From>/\n<From>/g;
$line =~ s/<Message/\n<Message/g;
$line =~ s/<\/Message>//g;
$line =~ s/<Text[^>]*>/\n/g;
$line =~ s/<\/Text>/\n/g;
$line =~ s/<Message //g;
$line =~ s/DateTime[^>]*>//g;
$line =~ s/<User FriendlyName=\"//g;
$line =~ s/\"\/>//g;
$line =~ s/<\/[^>]*>//g;
$line =~ s/<To>/\tTo: /g;
$line =~ s/<From>/From: /g;
$line =~ s/<[^>]*>//g;
print FILE $line;
}
close FILE;
```